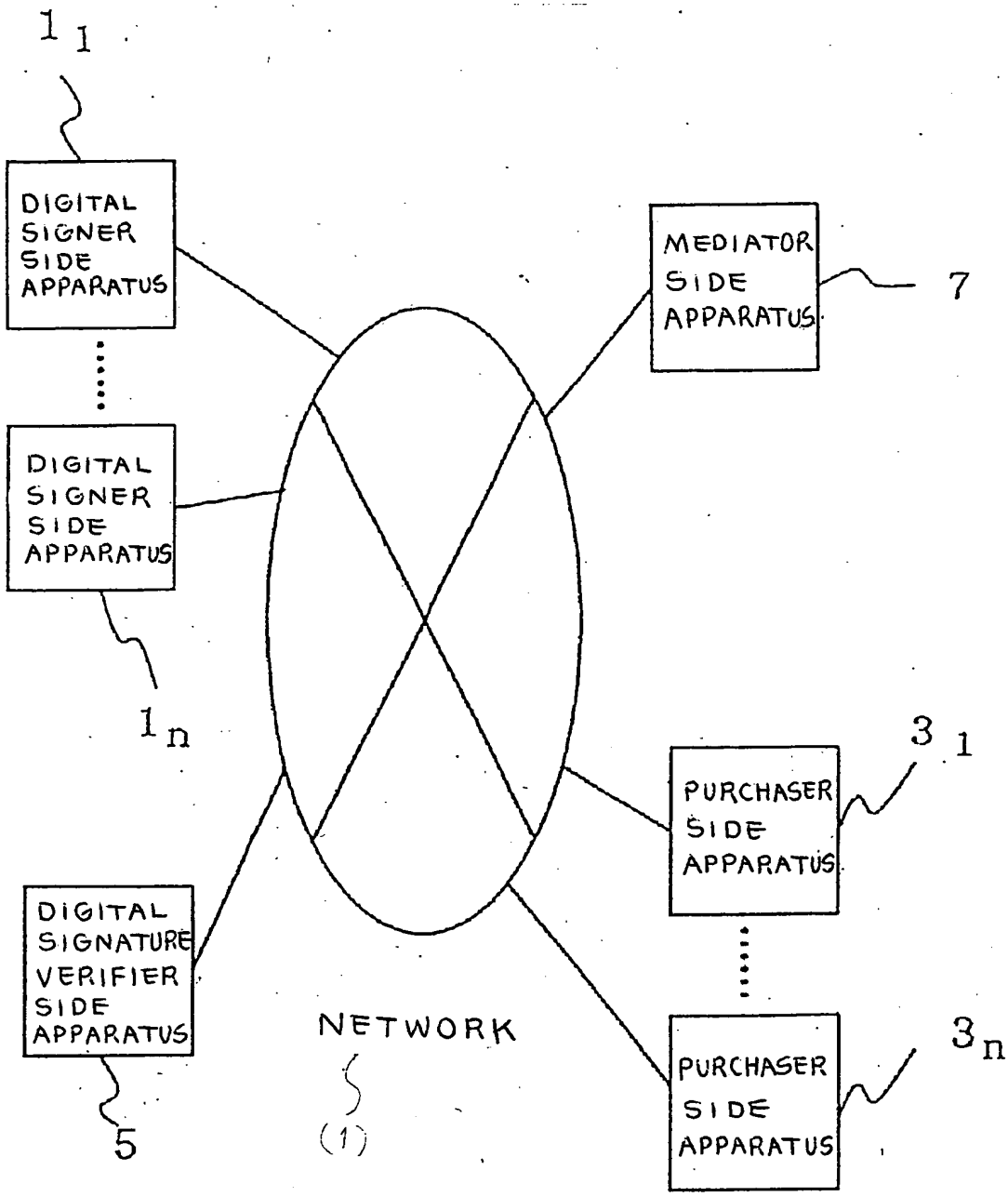
【書類名】 図面

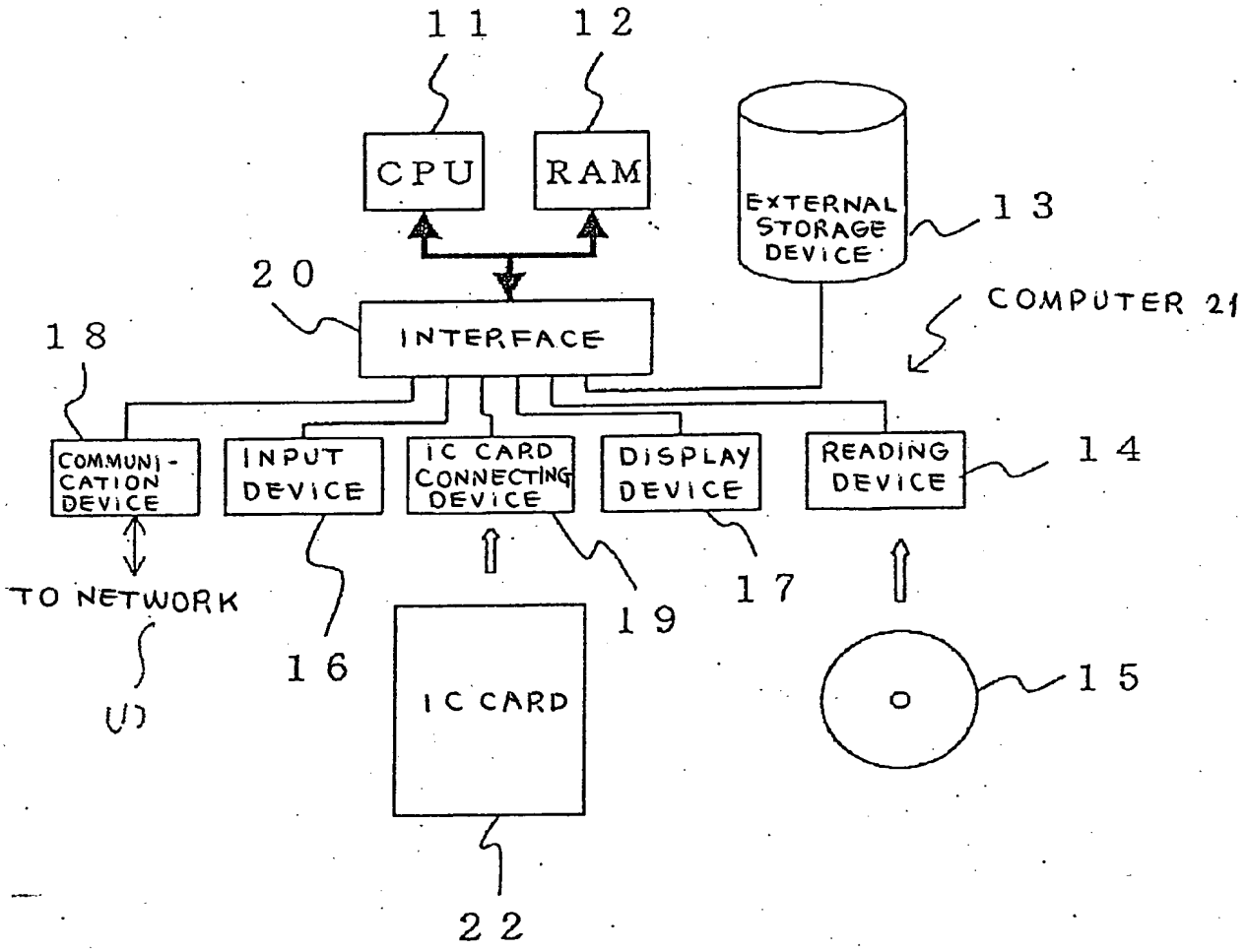
【図１】

FIG. 1



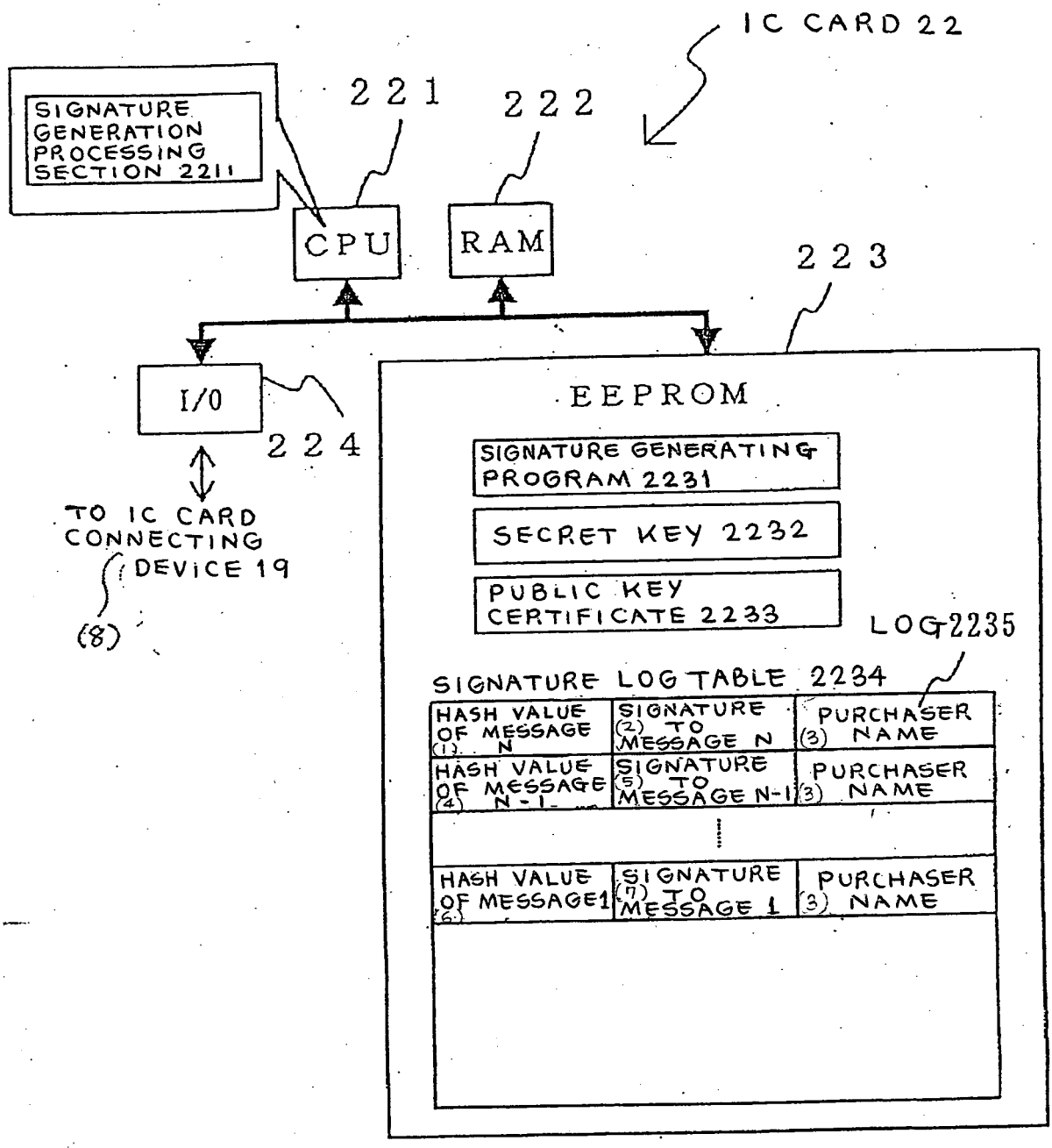
【図２】

FIG. 2


11
12
CPU
RAM
EXTERNAL STORAGE DEVICE
13
20
COMPUTER 21
18
INTERFACE
COMMUNI-CATION DEVICE
INPUT DEVICE
IC CARD CONNECTING DEVICE
DISPLAY DEVICE
READING DEVICE
14
TO NETWORK
16
19
17
IC CARD
15
22

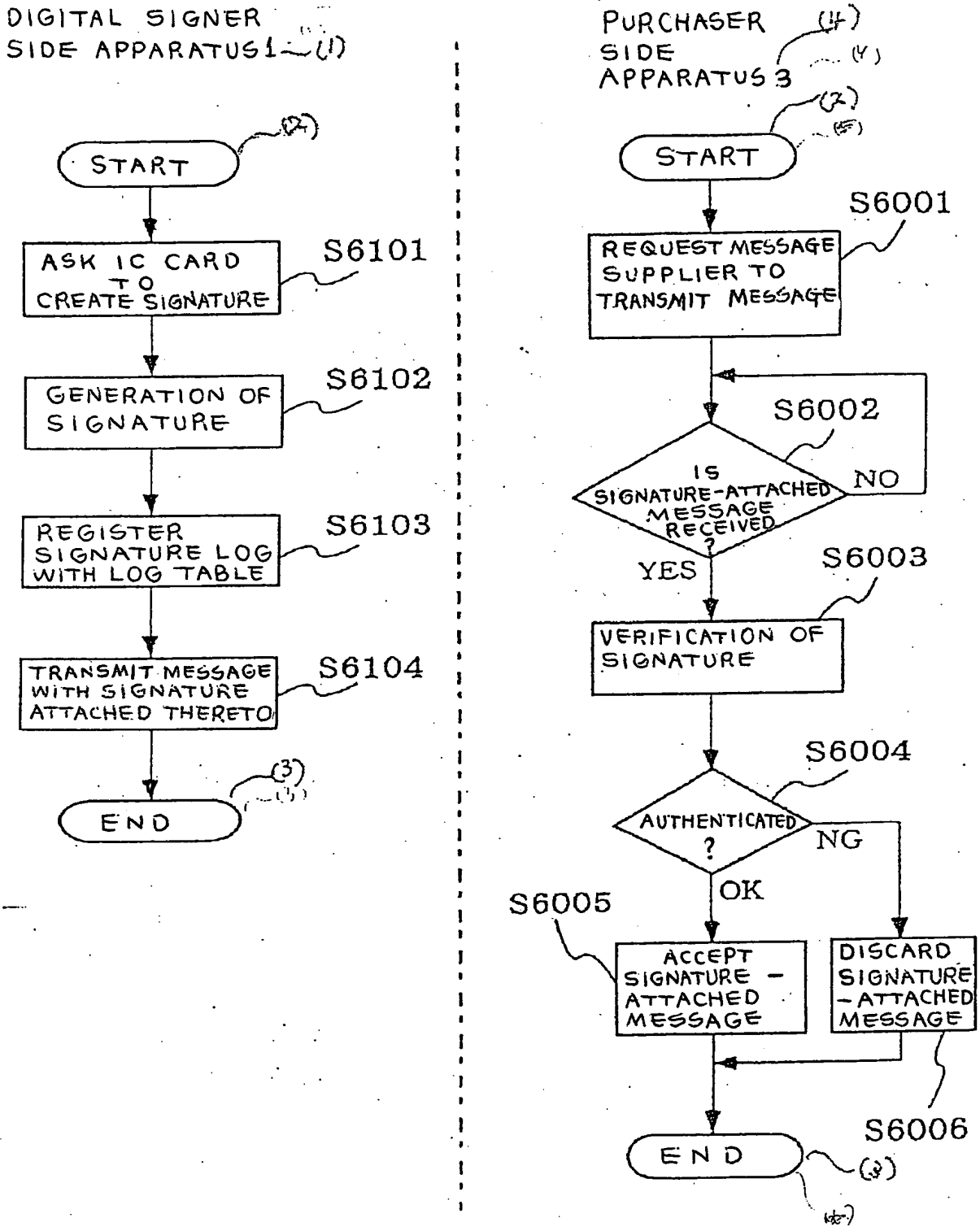
【図３】

FIG. 3


IC CARD 22
SIGNATURE GENERATION PROCESSING SECTION 2211
221
222
CPU
RAM
223
I/O
224
TO IC CARD CONNECTING DEVICE 19
(8)
EEPROM
SIGNATURE GENERATING PROGRAM 2231
SECRET KEY 2232
PUBLIC KEY CERTIFICATE 2233
LOG 2235
SIGNATURE LOG TABLE 2234
HASH VALUE OF MESSAGE N (1)
SIGNATURE TO MESSAGE N (2)
PURCHASER NAME (3)
HASH VALUE OF MESSAGE N-1 (4)
SIGNATURE TO MESSAGE N-1 (5)
PURCHASER NAME (3)
HASH VALUE OF MESSAGE1 (6)
SIGNATURE TO MESSAGE 1 (7)
PURCHASER NAME (3)

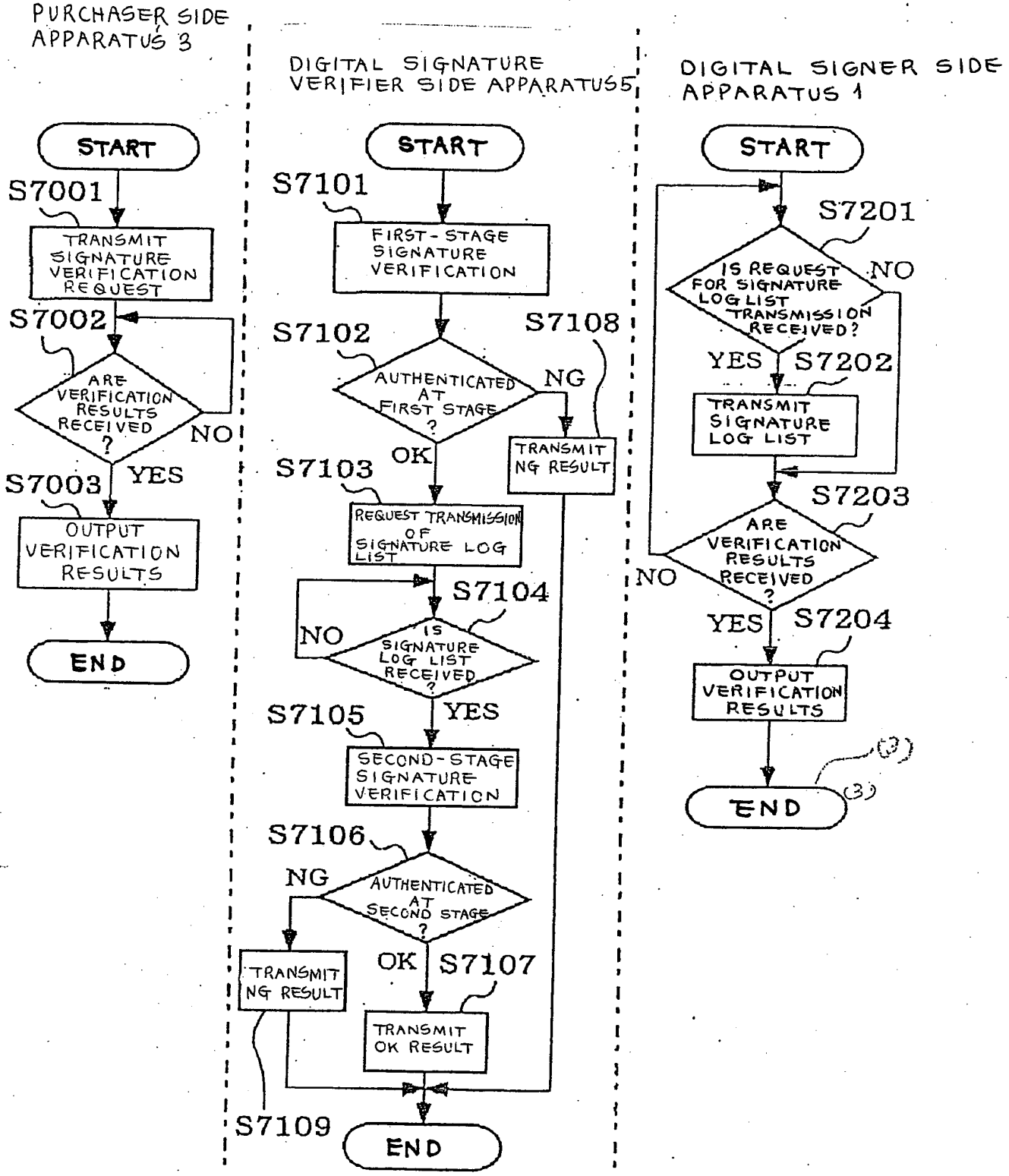
〔図４〕

FIG. 4


DIGITAL SIGNER SIDE APPARATUS 1
START
ASK IC CARD TO CREATE SIGNATURE
S6101
GENERATION OF SIGNATURE
S6102
REGISTER SIGNATURE LOG WITH LOG TABLE
S6103
TRANSMIT MESSAGE WITH SIGNATURE ATTACHED THERETO
S6104
END
PURCHASER SIDE APPARATUS 3
START
REQUEST MESSAGE SUPPLIER TO TRANSMIT MESSAGE
S6001
S6002
IS SIGNATURE-ATTACHED MESSAGE RECEIVED ?
NO
YES
S6003
VERIFICATION OF SIGNATURE
S6004
AUTHENTICATED ?
NG
OK
S6005
ACCEPT SIGNATURE - ATTACHED MESSAGE
DISCARD SIGNATURE - ATTACHED MESSAGE
S6006
END

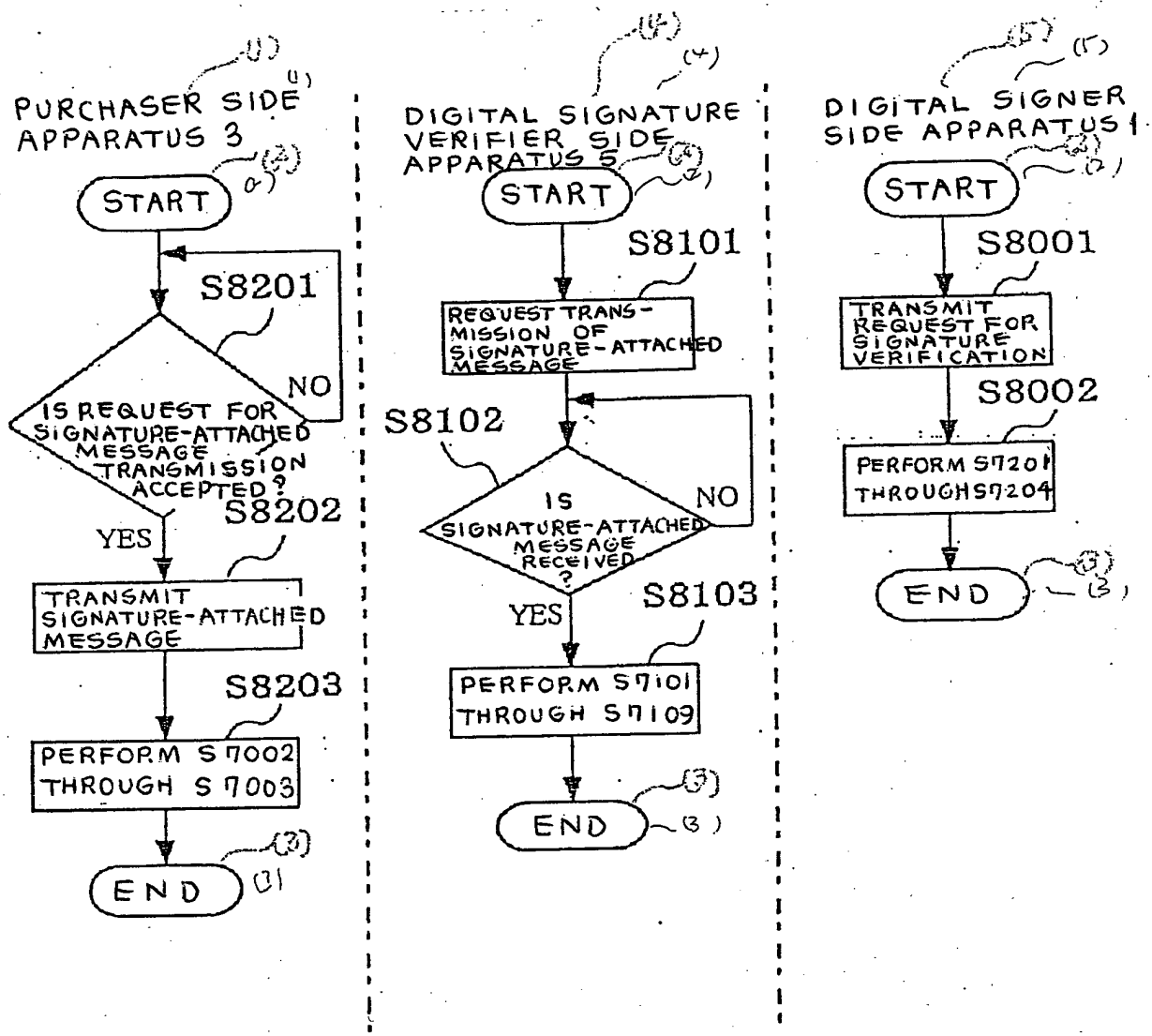
【図５】

FIG. 5


PURCHASER SIDE APPARATUS 3
DIGITAL SIGNATURE VERIFIER SIDE APPARATUS5
DIGITAL SIGNER SIDE APPARATUS 1
START
S7001
TRANSMIT SIGNATURE VERIFICATION REQUEST
S7002
ARE VERIFICATION RESULTS RECEIVED ?
NO
YES
S7003
OUTPUT VERIFICATION RESULTS
END
START
S7101
FIRST-STAGE SIGNATURE VERIFICATION
S7102
AUTHENTICATED AT FIRST STAGE ?
NG
S7108
TRANSMIT NG RESULT
OK
S7103
REQUEST TRANSMISSION OF SIGNATURE LOG LIST
S7104
NO
IS SIGNATURE LOG LIST RECEIVED ?
YES
S7105
SECOND-STAGE SIGNATURE VERIFICATION
S7106
NG
AUTHENTICATED AT SECOND STAGE ?
TRANSMIT NG RESULT
OK
S7107
TRANSMIT OK RESULT
S7109
END
START
S7201
IS REQUEST FOR SIGNATURE LOG LIST TRANSMISSION RECEIVED?
NO
YES
S7202
TRANSMIT SIGNATURE LOG LIST
S7203
ARE VERIFICATION RESULTS RECEIVED ?
NO
YES
S7204
OUTPUT VERIFICATION RESULTS
(3)
END
(3)

【図６】

FIG. 6


PURCHASER SIDE APPARATUS 3
START
S8201
IS REQUEST FOR SIGNATURE-ATTACHED MESSAGE TRANSMISSION ACCEPTED?
NO
YES
S8202
TRANSMIT SIGNATURE-ATTACHED MESSAGE
S8203
PERFORM S7002 THROUGH S7003
END
DIGITAL SIGNATURE VERIFIER SIDE APPARATUS 5
START
S8101
REQUEST TRANSMISSION OF SIGNATURE-ATTACHED MESSAGE
S8102
IS SIGNATURE-ATTACHED MESSAGE RECEIVED?
NO
YES
S8103
PERFORM S7101 THROUGH S7109
END
DIGITAL SIGNER SIDE APPARATUS 1
START
S8001
TRANSMIT REQUEST FOR SIGNATURE VERIFICATION
S8002
PERFORM S7201 THROUGH S7204
END

0807071 EP2234340

FIG. 7

SIGNATURE LOG TABLE 2234

2235

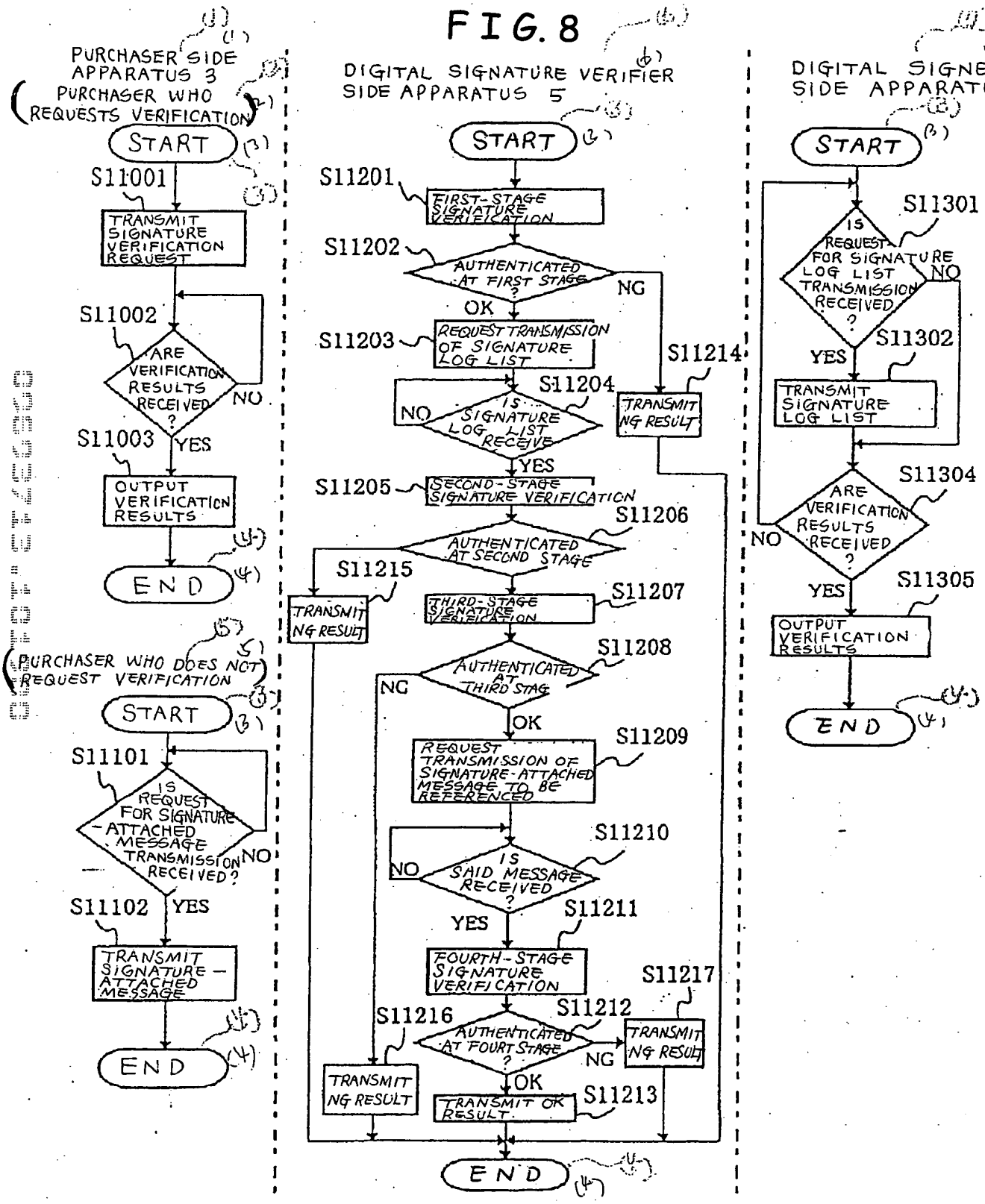
(1)	(2)	(3)	(4)
(1) PREVIOUS DATA P_{N-1} $(h(M_{N-1}), Sign_{N-1})$	(2) HASH VALUE $h(M_N)$ OF MESSAGE M_N	(3) SIGNATURE $Sign_N$ TO (PREVIOUS DATA P_{N-1}, MESSAGE M_N)	(4) PURCHASER NAME
(5) (5) PREVIOUS DATA P_{N-2} $(h(M_{N-2}), Sign_{N-2})$	(6) HASH VALUE $h(M_{N-1})$ OF MESSAGE M_{N-1} (6)	(7) (7) SIGNATURE $Sign_{N-1}$ TO (PREVIOUS DATA P_{N-2}, (9) MESSAGE M_{N-1})	(4) PURCHASER NAME
(8) (8) PREVIOUS DATA P_1 $(h(M_1), Sign_1)$	(9) (9) HASH VALUE $h(M_2)$ OF MESSAGE M_2	(10) (10) SIGNATURE $Sign_2$ TO (PREVIOUS DATA P_1, MESSAGE M_2)	(4) PERCHASER NAME
(11) (11) INITIAL VALUE IV	(12) (12) HASH VALUE $h(M_1)$ OF MESSAGE M_1	(13) (13) SIGNATURE $Sign_1$ TO (INITIAL VALUE IV, MESSAGE M_1)	(4) PERCHASER NAME

【図7】

ファイル=05123727001

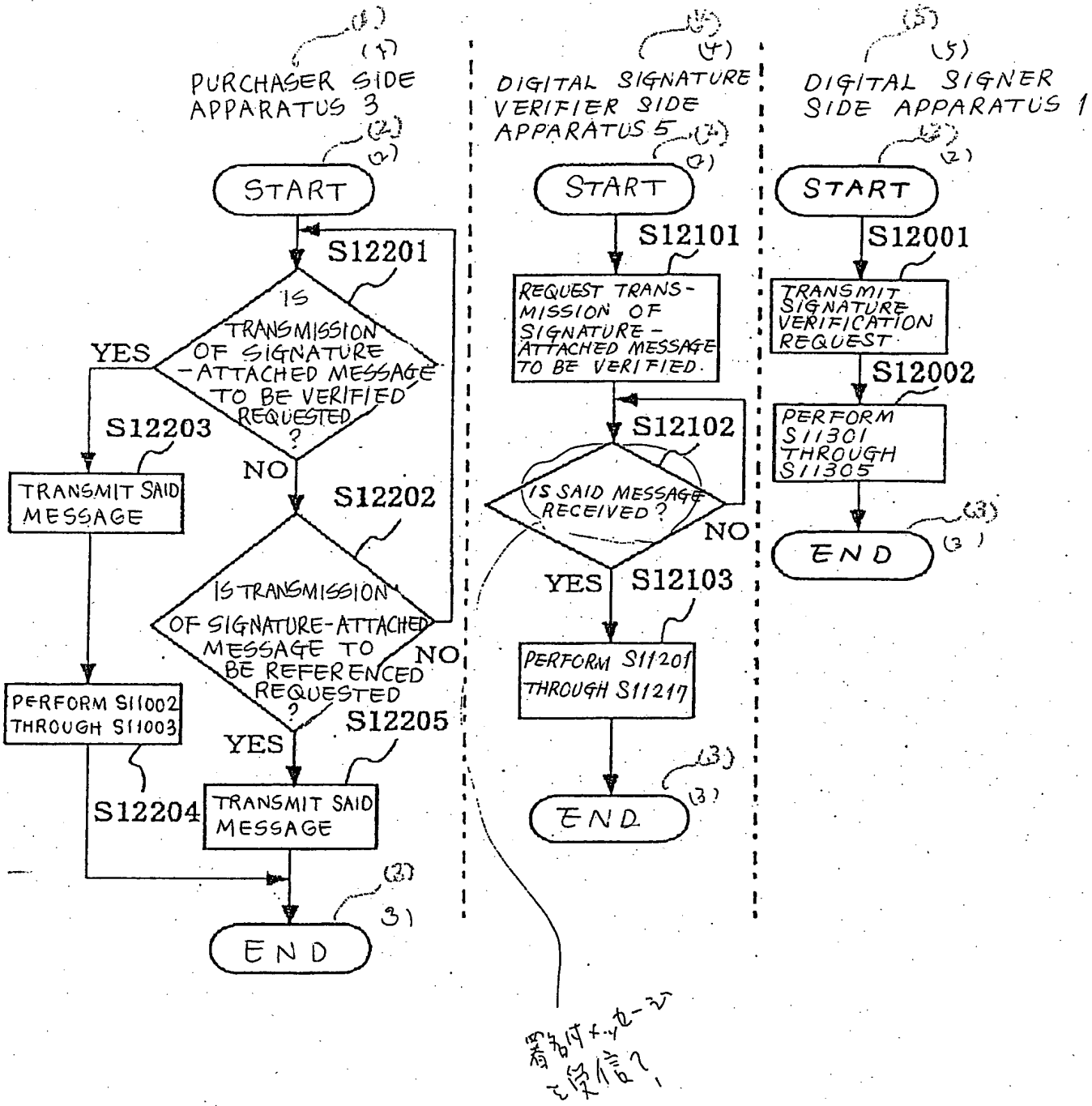
【図８】

FIG. 8


PURCHASER SIDE APPARATUS 3
PURCHASER WHO REQUESTS VERIFICATION
START
S11001
TRANSMIT SIGNATURE VERIFICATION REQUEST
S11002
ARE VERIFICATION RESULTS RECEIVED ?
NO
YES
S11003
OUTPUT VERIFICATION RESULTS
END
PURCHASER WHO DOES NOT REQUEST VERIFICATION
START
S11101
IS REQUEST FOR SIGNATURE-ATTACHED MESSAGE TRANSMISSION RECEIVED?
NO
YES
S11102
TRANSMIT SIGNATURE-ATTACHED MESSAGE
END
DIGITAL SIGNATURE VERIFIER SIDE APPARATUS 5
START
S11201
FIRST-STAGE SIGNATURE VERIFICATION
S11202
AUTHENTICATED AT FIRST STAGE ?
NG
OK
S11203
REQUEST TRANSMISSION OF SIGNATURE LOG LIST
S11204
IS SIGNATURE LOG LIST RECEIVED
NO
YES
S11205
SECOND-STAGE SIGNATURE VERIFICATION
S11206
AUTHENTICATED AT SECOND STAGE
S11207
THIRD-STAGE SIGNATURE VERIFICATION
S11208
AUTHENTICATED AT THIRD STAGE
NG
OK
S11209
REQUEST TRANSMISSION OF SIGNATURE-ATTACHED MESSAGE TO BE REFERENCED
S11210
IS SAID MESSAGE RECEIVED ?
NO
YES
S11211
FOURTH-STAGE SIGNATURE VERIFICATION
S11212
AUTHENTICATED AT FOURT STAGE ?
NG
OK
S11213
TRANSMIT OK RESULT
S11214
TRANSMIT NG RESULT
S11215
TRANSMIT NG RESULT
S11216
TRANSMIT NG RESULT
S11217
TRANSMIT NG RESULT
END
DIGITAL SIGNER SIDE APPARATUS 1
START
S11301
IS REQUEST FOR SIGNATURE LOG LIST TRANSMISSION RECEIVED ?
NO
YES
S11302
TRANSMIT SIGNATURE LOG LIST
S11304
ARE VERIFICATION RESULTS RECEIVED ?
NO
YES
S11305
OUTPUT VERIFICATION RESULTS
END

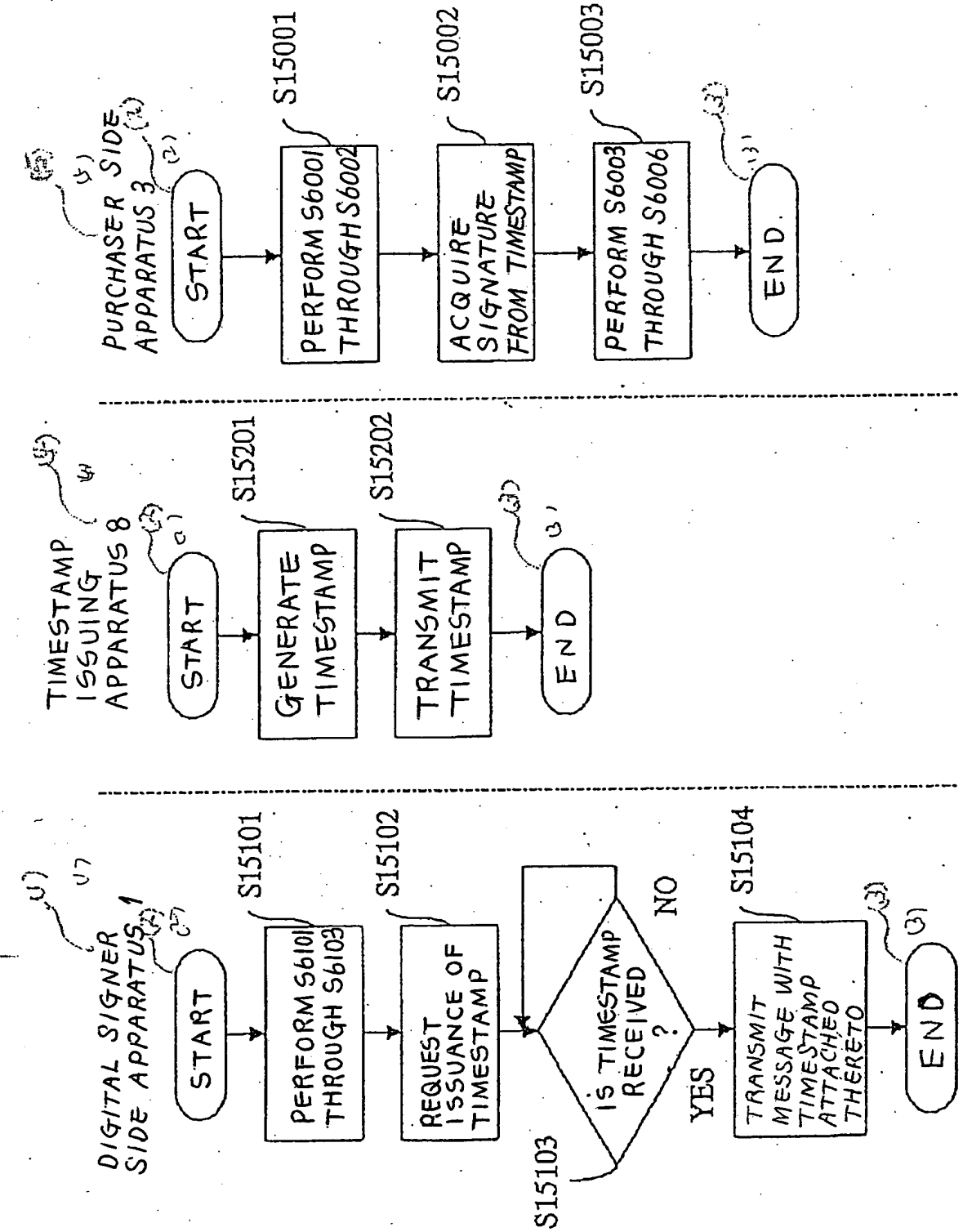
【図９】

FIG. 9


PURCHASER SIDE APPARATUS 3
DIGITAL SIGNATURE VERIFIER SIDE APPARATUS 5
DIGITAL SIGNER SIDE APPARATUS 1
START
S12201
IS TRANSMISSION OF SIGNATURE-ATTACHED MESSAGE TO BE VERIFIED REQUESTED ?
YES
NO
S12203
TRANSMIT SAID MESSAGE
S12202
IS TRANSMISSION OF SIGNATURE-ATTACHED MESSAGE TO BE REFERENCED REQUESTED ?
NO
YES
S12205
TRANSMIT SAID MESSAGE
PERFORM S11002 THROUGH S11003
S12204
END
S12101
REQUEST TRANSMISSION OF SIGNATURE-ATTACHED MESSAGE TO BE VERIFIED.
S12102
IS SAID MESSAGE RECEIVED ?
NO
YES
S12103
PERFORM S11201 THROUGH S11217
END
S12001
TRANSMIT SIGNATURE VERIFICATION REQUEST
S12002
PERFORM S11301 THROUGH S11305
END

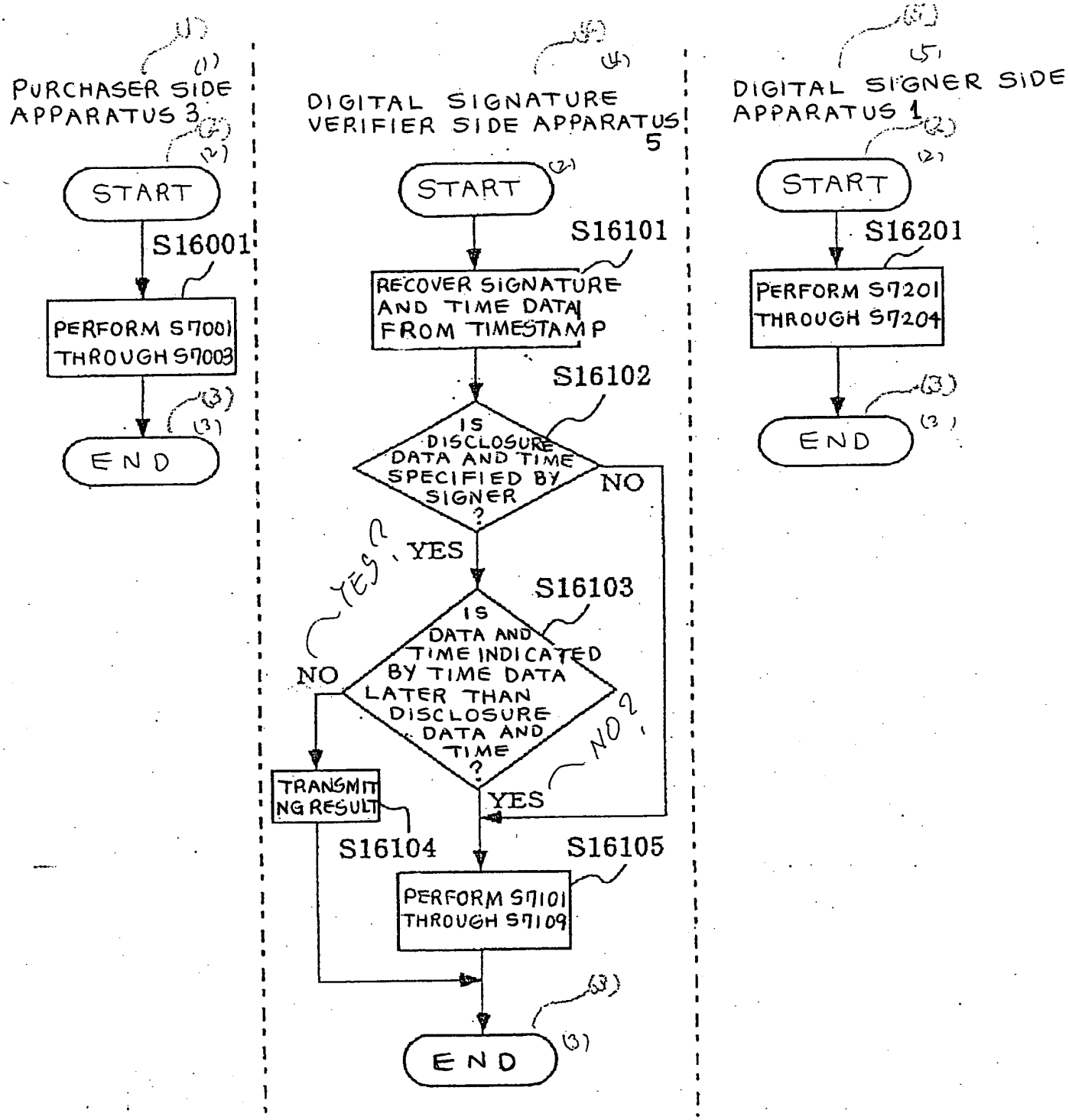
【図１０】

FIG. 10


DIGITAL SIGNER SIDE APPARATUS 1
START
S15101
PERFORM S6101 THROUGH S6103
S15102
REQUEST ISSUANCE OF TIMESTAMP
S15103
IS TIMESTAMP RECEIVED ?
NO
YES
S15104
TRANSMIT MESSAGE WITH TIMESTAMP ATTACHED THERETO
END
TIMESTAMP ISSUING APPARATUS 8
START
S15201
GENERATE TIMESTAMP
S15202
TRANSMIT TIMESTAMP
END
PURCHASER SIDE APPARATUS 3
START
S15001
PERFORM S6001 THROUGH S6002
S15002
ACQUIRE SIGNATURE FROM TIMESTAMP
S15003
PERFORM S6003 THROUGH S6006
END

【図１１】

FIG. 11


PURCHASER SIDE APPARATUS 3
START
S16001
PERFORM S7001 THROUGH S7003
END
DIGITAL SIGNATURE VERIFIER SIDE APPARATUS 5
START
S16101
RECOVER SIGNATURE AND TIME DATA FROM TIMESTAMP
S16102
IS DISCLOSURE DATA AND TIME SPECIFIED BY SIGNER ?
NO
YES
S16103
IS DATA AND TIME INDICATED BY TIME DATA LATER THAN DISCLOSURE DATA AND TIME ?
NO
YES
TRANSMITTING RESULT
S16104
S16105
PERFORM S7101 THROUGH S7109
END
DIGITAL SIGNER SIDE APPARATUS 1
START
S16201
PERFORM S7201 THROUGH S7204
END

【図１２】

FIG. 12

SIGNATURE LOG TABLE 2234

2235

HASH VALUE OF MESSAGE N	SIGNATURE TO MESSAGE N	PURCHASER NAME	TIMESTAMP
HASH VALUE OF MESSAGE N-1	SIGNATURE TO MESSAGE N-1	PURCHASER NAME	NO ENTRY
⋮			
HASH VALUE OF MESSAGE N-m	SIGNATURE TO MESSAGE N-m	PURCHASER NAME	TIMESTAMP
HASH VALUE OF MESSAGE N-m-1	SIGNATURE TO MESSAGE N-m-1	PURCHASER NAME	NO ENTRY
⋮			
HASH VALUE OF MESSAGE 2	SIGNATURE TO MESSAGE 2	PURCHASER NAME	NO ENTRY
HASH VALUE OF MESSAGE 1	SIGNATURE TO MESSAGE 1	PURCHASER NAME	TIMESTAMP